THE HISTORY OF HUT 6

IN THREE VOLUMES

VOL. II

1.813 S.S. AND POLICE KEYS

1.8130 General Characteristics

The S.S. keys formed a relatively small X but in many respects very interesting group. While a branch of Army keys in the wider sense and for this reason dealt with by the Army section in the final Air/Army division of Hut 6, they showed certain peculiarities which differentiated them not only from Air keys but from most other Army keys. These were

(a)specialised content and style. The keys used many contract--ions not commonly met with on pure Army traffic e.g. the most common abbreviation was XSSX which on Army keys was often indicated by SIEGFRIED SIEGFRIED. The use of "spellers" was very rare on S S. keys and the use of X as a stop or after a contraction very common. YY was rare and wahlworts were never used.

(b)individual rules of keys in certain respects (see the sections on this topic). It seems probable that the keys were made up and distributed by a special S.S. cipher office.

(c)fixed callsigns on the bulk of the traffic throughout normally OL., OM., or DO.. This made W/T research and traffic identification much simpler on S.S. keys than on the Army proper. And if there were cribs there was no trouble in identifying the relevant messages.

1.8131 History to the End of 1941

During the war the first S.S. key to be broken was Orange -- known to the Germans as the S.S. Stabsmaschinenschlüssel -- though it was not a staff key in the normal Army sense and the traffic was not as a rule "top secret". The content was S.S. matter of a general administrative nature, including organisation of concentrat--ion camps.

The early history of the breaking of Orange to May 1941 has been already referred to. Up to the end of 1941 the position remained essentially unchanged: Orange still cillied occasionally and was broken at intervals on bombe menus or hand attempts. From the beginning of M.R.2 Orange was one of the most interesting colours and was one of the first to be formally adopted; but it must be admitted that it was hard enough going.

Apart from Orange two other S.S. keys had appeared before the end of 1941. The first was the famous T.G.D.θ, the key of the Security Police. From information we have received this key was broken by the Poles as far back as 1937 but the only decodes Hut 6 was able to examine were on July 31, 1939, when the traffic was largely in code. The key was never broken during the war and to this day is one of the classic mysteries of Hut 6. It never cillied so far as we know and no convincing re-encodement from any other key was ever produced.

The other key was named Orange II. It first appeared in December 1941 but had not been broken by the end of the year. It

X For list of keys (mainly fruit names) see general Army list There were never more than a dozen separate keys.
θ Named after the Berlin callsign at one period. Later T.G.D. used fixed callsings of the type SN., SO..

used Orange-like calls but had a separate series of discriminants which in January 1942 it began repeating day for day.

1.8132 1942: The Orange Age

1942 heralded an era of discoveries. Orange I began to be broken more frequently on cillies particularly an amusing type of cilli from one station OMW -- the famous AAA variety. Increasing decode evidence threw up some crib possibilities of which more hereafter.

On Orange II success was also gained in February and it was proved that December, January and February were all on the same key.* This meant that one could take corresponding days together and combine both cillies and ringstellung tips, a fascinating pursuit which resulted eventually in the breaking of a substantial number of days of the first cycle. Orange II was found to deal mainly with communications between Berlin and S.S. divisions on the Eastern Front with the well-known LSSAH and the Wiking Division figuring prominently.

4152 Meanwhile an intriguing mystery was revealed on Orange I. In February 1942 a new frequency 4152 came up with Orange calls and discriminants but was obstinately dud on the Orange key. This phenomenon aroused interest and some disquiet; for never previously had the same discriminant on the same day failed to decode on the same key. As nothing was known of the new frequency, nothing could be done in the crib line; but in March 1942 two cillies turned up on 4152 on a day when the main key was broken and the cillies were rodded out on the Orange stecker. The wheelorder was the same as the main key but the ringstellung differed: no connection was ever found. But on the evidence of signatures it was almost always possible to rod out the 4152 when the main key was known and more rarely the 4152 was broken first as a stepping-stone to the main key.

HOR-HUG Reports The contents of 4152 Orange dealt with some of the concentration camps that have since attained notoriety, (such as Auschwitz, Dachau, Oranienburg), and the next sensational advance in S.S. cryptography was also connected with this frequency. For several months a number of non-enigma messages had been sent out from some six or seven stations to Berlin early in the morning -- in fact between 7 and 8 a.m. These messages were eventually passed on to us as it was thought they might tie up in some way with the Enigma traffic. Inspection revealed the following characteristics. The messages, known as HOR-HUG reports from two frequently occuring code groups, were short, consisting of about ten groups of letters, followed by a few more or less invariable code groups. In the message proper the number of letters in any group never exceeded four, and on any one day only ten different letters were used. The last point strongly suggested a figure code and on this hypothesis one day's traffic was broken early in April 1942. The messages contained in tabular form the vital statistics of concentration camps: the first four columns denoted (A) number of inmates at start of previous day, (B) new arrivals, (C) departures by any means, (D) number at end of day. Thus A+B-C=D, and for any station D on one day was A on the next. Once this was known it was generally easy to break any individual day on its own by a series of equations, and it was, of course, absurdly simple if the previous day's substitution was known.

* It was later discovered that the key was still used in March and this period was called the first cycle. The second cycle lasted from April till Orange II died out in August.

The cryptographic importance of this discovery lay in the remarkable fact that the substitution was derived from the Orange stecker of the day by the simple process of writing the numbers 1,2,3...0 above the first five stecker pairings.X Fortunately this incredible piece of enemy carelessness was noticed as soon as the first figure code had been broken, and no time was lost in exploiting it. Arrangements were made at once to have the vital messages well intercepted and the HOR-HUG key was broken as early as possible in M.R.1. Thereafter the Orange stecker for the day was known.

This knowledge could be used to aid breaking in three distinct ways: (a) by rodding a crib, beginner or signature or sometimes a cilli;0 (b) by using the known stecker in hand attempts on cillies plus ringstellung tip or (c) by running bombe menus on either cillies or cribs with the known stecker postulated. Method (b) was the most elegant and the fact that in hand attempts one could nearly always start from a known stecker pairing made it possible to try a far larger number of positions than would otherwise have been feasible. Other factors in favour of the hand break method were that the HOR-HUG stecker made rejection of wrong stories easy and that the Army ringstellung rule (which Orange frequently obeyed) made it sometimes possible to guess the ringstellung even without a tip by Herivelismus.

Method (a) could be very laborious and was not as a rule adopted unless circumstances were favourable -- i.e. unless there was in close proximity a number of constatations where the stecker of both letters involved was known. Method (c) was a maid-of-all-work for use in cases where other lines of attack were impracticable or too laborious. It had the merit of cheapness in bombe hours as it could be run on the corner of a machine which was doing another job as well (for menus could be made up on a small number of links because of the extra closures) and it was possible to combine the method if desired with method (a) e.g. by putting down a favourable stretch on the rods and running another stretch on the bombe.

Henceforward for about a year the HOR-HUG stecker + formed the trump card of the Orange cryptographer. March and April 1942 were the best Orange months to date but from May 1942 to January 1943 an average of 19 days per month was broken. Orange was always a colour on which we looked for signatures, as virtually every message started with an address and ended with a signature: and though few of the signatures were really good for breaking in their own right, some were serviceable enough when the whole stecker was known (as in breaking the 4152) or when half the stecker was known. One of the best was from OMG:- XSPORRENBERG XSSX OBERSTUFX.

Orange Cribs But during 1942 a few real cribs were discovered on Orange. These were never quite first-rate by the standards of

X Each individual stecker pair was written in alphabetical order - not the whole set. Thus 2 was farther on in the alphabet than 1, 4 than 3, and so on.

0 For the technique of rodding in general and the somewhat special problems of rodding on half the stecker (instead of the complete stecker) see the appropriate chapter in the technical volume.

+ It should be mentioned that the HOR-HUG reports were not sent out on Sundays or public holidays such as Xmas Day: but to compensate there was hardly any Orange traffic on these days.

easier colours but were none the less very welcome on a colour normally so cribless as Orange and, of course, even a comparatively poor crib is greatly strengthened by the HOR-HUG stecker. The best-known of the Orange cribs were the Bestand and Weather messages.

The Bestände were messages similar in content to the HOR-HUG reports but enciphered in Enigma. There were two such messages, the men's and the women's Bestand, and both were summaries of the state of affairs at the concentration camp of Stutthof near Danzig The cribs had a usable stagger stretch and quite a good signature. (XKLX STUTTHOFX) and could often be used to break with the HOR-HUG stecker.

But the most famous of all Orange cribs were the Weather messages from Krakau (OLQ). The first of these messages turned up in October 1942 and they were at once recognized as high-class weather reports covering the whole of Europe. Apart from their value for our bombing operations, these reports were at that time of particular intelligence interest because the state of the weather on the Eastern Front was then regarded as of high importance in forecasting the developments of that crucial campaign and so a morning weather report on the Eastern Front was placed daily on the Prime Minister's desk. It was suggested that if Orange could be broken more or less currently -- at least before 8 a.m. the next day -- the Orange Weather could be included in this report.

Fortunately the message itself was both readily identifiable and proved cribbable in an original way. It was found to end SONNEN AUFGANG KRAKAU MORGEN.....UHR SONNEN UNTERGANG...UHR. Consultation of the Nautical Almanac revealed that Krakau was an extremely fortunately situated place with a longitude of 19° 59' which counted as 20° and made it easy to calculate the times of sunrise and sunset. These were found nearly always to agree with the German times,X and as a result on any weather message there was a stagger stretch of average length 50 -- ideal for breaking on the HOR-HUG stecker. Henceforward the Orange Weather or Sunrise at Krakau became the main means of breaking: and to secure currency M.R.1 took over partial responsibility for the key. This new crib was the more important as in August 1942 the AAA cillier had ceased to send traffic and though pronounceable and keyboard cillies still occurred on Orange at intervals no single station quite took the place of the deceased OMW.

Quince While Orange I was thus being broken on concentration camp statistics and astronomical lore -- a striking example of the cosmic aspect of cryptography -- Orange II had faded away to nothingness in the midst of its second cycle. But in August 1942 this blank began to be filled by a new S S. key named Quince destined in the latter half of the war to become the principal key of its class though this could not have been foreseen from its modest origins. Quince was called the S.S.Feldnachschubmaschinen-schlüssel and was primarily concerned with supply and administration of S.S. divisions wherever they were stationed: Eastern Front, Balkans, Italy and the West. While it never contained operational orders of the first importance, it did at times contain reports of operational interest e.g. a flamboyant description of one of the last noteworty German successes on the Eastern Front, the recapture of Kharkov, was sent in a long message on Quince on March 13, 1943.

X Later it was found that the Germans made occasional errors in caluclating the times.

The first Quince day to be broken -- on straight keyboards -- was August 27, 1942 and in September (which repeated discriminants and keys of August) more breaks were secured on cillies, ✕ sometimes eked out by beginners (ANX, ANX SSX or ANX SSX FHAX ⊖ were all worth trying). From October 1942 onwards Quince had a new key every month. It continued to be broken most frequently on cillies -- both pronounceables and nearnesses -- but occasionally on cribs. The earliest crib was called the Dodgemeldung -- a report from DOJ to DOF (Berlin) and it was first used in November 1942. In the course of the following year as cillies declined this crib was employed more and more frequently.

On December 30, 1942 Quince produced one of the best banbury stories on record. From the evidence of counts two 5-tl. messages and one 6-tl. had clearly used the same indicators, part for part, at least for the first four parts of each message: but it was impossible to arrive at the message settings by subtraction. The day came out on a pure banbury menu and the settings were found to be for the 5-tle

PRO SIT NEU JAH RXY

and for the 6-tle

PRO SIT NEU JAH RXA HOI.

With these good wishes ringing in our ears we set forth into 1943.

1.8133 1943-5: The Quince Age

Decline of Orange In 1943 though S.S. keys in general improved their position this was mainly due to the success of the newcomer, Quince; for blow after blow was suffered by Orange, the senior S.S. key. "The most unkindest cut of all" was dealt early in the year when towards the end of January it was announced that landlines were to be used instead of the vital frequency 4152. This decision was carried into effect forthwith and by February 1943 the HOR-HUG messages were no more.

The disappearance of the HOR-HUG stecker revealed the true weakness of the crib position on Orange and there was a catastrophic decline in the number of breaks. It is possible indeed that on a colour of the highest priority value we might by great extravagance in bombe time -- e.g. by running all possible variations of the Weather -- have made a supreme effort to maintain our hold. But Orange was not sufficiently important to justify such expense: when it had to compete on level terms -- i.e. without the bonus of the HOR-HUG stecker -- with colours of operational importance we soon discovered that the amount we could run was severely limited.

✕ A popular cilli in the early days was PFL followed by OCK or AUM in 2-tl.messages (PFLOCK and PFLAUM were S.S. officers).

⊖ FHA=FUEHRERHAUPTAMT.

† For completeness' sake it should be recorded that two minor S.S. keys, Orange III and Apple, existed for a comparatively brief period in 1942. Orange III dealt with the affairs of the S.S.Kav.Div. and was broken several times on cillies plus ANX (which was almost 100% on this key.) Apple from D/F evidence was used by S.S. groups in Norway. It gave a few fair cilli stories, and once even a re-encodement that was thought well of, but none the less never elected to come out.

There was never any permanent recovery from this loss though even in 1943 periods of moderate success occurred. Breaks could still be secured on cillies, beginners or signatures or on the Weather though even as a crib this deteriorated; latterly the times of sunrise and sunset were omitted. A new method of entry -- R.E.'s from Quince -- was also employed whenever possible.

June and July 1943 were both considered quite good months at the time. But even they only scored 9 and 6 breaks respectively and the monthly average of breaks from February to August 1943 was only 7 (as opposed to 19 in the previous nine months).

This unfortunate colour reached the nadir of its fortunes in September and October 1943 when a long-impending crisis in our cover resources came to a head and Orange had to be completely sacrificed by the removal of sets. In November it proved possible to restore cover and happily a quick break was achieved on keyboard cillies plus ANX SSX: but none the less by the end of the year Orange was far from convalescent and was indeed in a very delicate position. The few breaks that were achieved were due to cillies or R.E.s from Quince.

Revival of Orange: In the course of 1944 matters somewhat improved and in February a fair number of breaks was secured not only on cillies and R.E.'s but in some cases on new cribs of which the most interesting and best was the so-called "Bomb for Terboven". Terboven, the Reichkomissar in Norway, had a fatherly interest in Dusseldorf and liked to be informed whenever there had been a raid on that town and the address of this message could be used as a crib.

In March 1944 it was discovered that current Quince was repeating in a rather complicated pattern elements of the keys of January Orange, and this eventually led to the breaking of all January Orange. This, of course, gave much needed decode evidence and as cillies tended to become more frequent -- especially on 6535 -- a good deal of Orange was broken in the summer months. It was easy to break any day with a good cilli story :: it was in general very difficult and expensive to break days when there was not a good cilli story and much depended on the bombe position. Apart from a message like Bomb for Terboven Orange crib menus were usually on signatures -- not cribs in the strict sense -- and these were liable to frequent alteration: in any case owing to their shortness these jobs had generally to run as delayed hoppities on the Americal naval bombes which were subject to frequent jams. Hence Orange breaks would come in a rush due to a series of good cilli stories: then there might be a lull due to the absence of cillies while shots on signatures piled up in America. Eventually the jam would be released, probably a few breaks secured and the cycle would start anew.

The cilli stories -- which were mainly but not always strings of keyboards -- reached their height in July and August 1944. The piece de resistance was unquestionably this memorable sequence on August 4 -- PAQ, YSW, XDE, CFR, VWT, BHZ, NJU, MKI, LKO, MJI , NHU, BGZ, VFT, CDR, XSE, YAW. Breaking in this month was also facilitated by a curious stecker pattern from which it was possible on occasions to predict the self-steckered letters for the day.

Final Position: On September 15, 1944 the CY device began to be used on S.S. keys. As is now known by captured documents, the Germans introduced CY and random indicators at the same time. To this cause we must probably assign the sudden death of Orange cillies.

From this time on Orange went into a cryptographic decline. Two

fair means of breaking were left: (1) variants of AN ALLE FUNK-STELLEN on CQ messages and (2) a good signature from OLD known as the Teschner signature. But nothing else that was any use could be discovered: and so when these last cribs died in the course of nature (for all cribs are mortal) Orange breaking stopped. The only remaining days broken were on a stray R.E. from Quince and on long shots such as BETRIEBSSPRUQ in what looked like a signals/messages Such isolated breaks showed no real possibilities of new progress.

There was, however, to be a last glimpse of Orange before the end. The keys for April were captured and it was possible to decode the full month's traffic. Cryptographically the position was all but impossible: there were no cribs nor even reasonably good signatures and a formal attempt to break the scanty remnants of May Orange on the evidence of April was foredoomed to failure.

Golden Age of Quince It is a relief to turn from the rather melancholy story of Orange and the anticlimax in which it ends to the happier tale of Quince -- a colour which especially in the last eighteen months of the war had such consistent and uninterrupted success that at times it was almost dull. Yet happy is the key that has no history.

It is, however, possible to divide the story of Quince into three successive stages which overlap to some extent but are yet broadly distinguishable. In the first period (which has been already discussed) Quince was broken mainly on cillies. But in the course of 1943 a gradual but persistent decline in the frequency of cillies took place and cribs were used more constantly and from July to November 1943 Quince can be more fairly reckoned a crib colour. The old crib, the Dodgemeldung, was still frequently employed and a new arrival, the Eugenmeldung, a report from the S.S. Div. Prinz Eugen, then stationed in the Balkans, to the S.S. FHA at Berlin, proved a valuable second string. This message has a curious and complicated history: it was at various times passed on Quince, Raven, Wryneck and Peregrine, and sometimes it was possible to break Quince on R.E.s from these keys.

The third and last stage in the history of Quince began in November 1943 when the frequency 6315/3851 which carried the Balkan and Italian Quince suddenly packed up. This involved the disappearance of the Eugenmeldung and left Quince cribless, as the Dodgemeldung had already gone. Henceforward apart from occasional breaks on cillies we had to rely on beginners and signatures and Quince soon became a classic example of this type of key. It was broken almost daily to the end of the war on addresses such as ANX SSX FHAX INX SIEBENX, signatures such as the famous pair SCHEFTEL and SCHAEFER, and a host of others. This was an expensive process but Quince (which in 1944 steadily increased in quantity and quality) was counted well worth the cost and success was virtually certain to reward perseverance.

Occasional cribs would sometimes appear for a fortnight or so but rarely for longer: there was probably no key which was broken so often that had so few genuine cribs. The paradox about Quince is that its last eighteen months must have been the most interesting to Hut 3 and the dullest to Hut 6: for breaking by sledgehammer methods has none of the elegance and finesse dear to the cryptographer's heart. But Quince's intelligence importance was at length recognised by its promotion to full Watch status in December 1944.

The Quince keys for April and May 1945 were captured in a great S.S. key haul towards the end of the war: and as the Germans got into a complete muddle about what was compromised and what was not, no new

key was issued and we were able to decode Quince currently to the end. This was not so valuable as it may sound as traffic fell drastically and there were sometimes only one or two messages a day. But Hut 6 never looked gift horses in the mouth and in fact the very lack of traffic made it in one sense more desirable for us to have the key as otherwise we would have had difficulty in breaking it.

Like Orange and indeed all the S.S. keys, Quince ends in a cryptographic anticlimax: but we could at least claim that it remained breakable as long as there was any quantity of traffic. Probably no Research key (for such it was for most of its life) was more frequently or regularly broken: let this be its epitaph.

Minor S.S. Keys A large number of minor and sometimes more or less ephemeral keys - not always easy to identify - were thrown up by the S.S. system from time to time, and deserve brief individual mention.

Two keys were both confusingly called Quince II, though they had in reality no connection with each other. One was used by certain S.S. units in Italy and the Balkans and was first broken on a remarkable cilli story - seven HRD's - on October 13, 1942. This was probably the first appearance of the key. It was later broken a few more times on cillies or signatures but disappeared in November with the rest of Balkan and Italian Quince.

The second Quince II was more reasonably named. It was the S.S. Chef Sonderschlüssel and the traffic was nearly all "Top Secret". In fact, the orthodox and almost universal method of breaking was to run variants of the beginning GEHEIMEKOMMANDO-SAQE on any message, preferably long part messages, though there were a few sporadic cribs. Quince II in this new sense was first broken on April 1, 1944 under the name of Discriminating Quince. To the end nearly all its messages discriminated, and this was indeed the only way by which either the Germans or ourselves could distinguish the messages from Quince I.

Another Balkan key (like the first Quince II) was Peregrine,* which had a brief life from August to October 1943. It was used by the S.S. Div. Prinz Eugen and passed the Eugen-meldung and usually nothing more. Its intelligence value was negligible as this message was in any case often read on other keys: but it had some cryptographic importance as a possible lead into Quince or Balkan Army keys. It was always broken on the Eugenmeldung used either as a crib or a R.E. from some other key. One peculiarity was that in September (though not in August or October) every key broken had eleven stecker pairs - a fact which suggests the keys were home-made. It is also worthy of note that the version of the Eugenmeldung passed on Peregrine was sent to the V S.S. Geb. Korps and the reason for the decease of Peregrine was that this corps and the Prinz Eugen division came together in the same place.

In 1944 there appeared a trio of keys named Medlar, Grapefruit and Pumpkin. Medlar was originally called the Quince-Orange Link (German name S.S. Querverkehrschlüssel) and was definitely intended for pass-on messages between the

* This key was given a bird name before its true nature was known.

Quince and Orange systems - presumably as a means of avoiding R.E.'s. There was seldom much traffic on this key and what there was was very hard to distinguish from Quince and Orange: so it was never blisted separately (except in April and May 1945 when discriminants and keys were known by capture), and broken rarely, generally by accident. Medlar was first broken on May 29, 1944 and from the German key-number this month was the first in which it was used; it continued till the end of the war and in fact Medlar May 9, 1945 was the latest key on which traffic was decoded.

Grapefruit was a concentration camp key - a revival of 4152 Orange on the old frequency but on this occasion with a key of its own and - alas - without the HOR-HUG stecker of the past. This key used fixed DO, callsigns and appeared in April 1944. It was only broken once on August 21, 1944 when a double R.E. from Quince and Orange came out after immense efforts. The traffic was virtually uncribbable; the only line of attack was on CQ messages which in any case had an extensive repertory of varied forms. Grapefruit gradually declined and was practically dead sometime before the end of the war.

Pumpkin was a propaganda key connecting Rome and later North Italy with Berlin. It started in April 1944 when the break of one day on cillies revealed that the key was identical with the Quince I key of the previous month. Also May Pumpkin used the same key as April Quince. But the repeat of keys did not continue thereafter and no more Pumpkin was broken. It must be admitted that no attempts were made: the contents of the traffic were so valueless that Hut 3 was apt to despise Pumpkin even when it was secured as a free gift. The later history of Pumpkin is like Grapefruit except that is decline and final disappearance were even quicker.

In the closing stages of the war a new key, Plum, (S.S. M/S Sondersatz C) supplanted Quince I for a short period during a compromise and was broken for several days in March 1945 on Quince cribs. When a new Quince key had been distributed, however, Plum declined and indeed was only broken once more on a R.E. from Quince when only about half a dozen messages decoded.

Also in the last stages a considerable haul of S.S. keys gave us the Orange, Quince I, Quince II and Medlar keys for April and all the above (except Orange) for May[K]. Of all this bunch of keys Quince II was the most useful to intelligence and indeed it produced some sensational messages in the last agony of the Reich, in particular, the news of Görings arrest (by Himmler?) and a long message of indignant expostulation sent by Marshal to Führer. Incidentally the capture of these keys with their discriminants immeasureably simplified the sorting problem: for some time past we had been reduced to a composite S.S. Discriminating blist which contained a large number of keys - Quince II, Quince I Discriminating if any, Orange Discriminating if any, Plum, Medlar and so on.

Apart from the keys already referred to there were broken from time to time odd unidentifiable keys to which were given such names as Quince III, Orange II for want of better and two keys that are referred to in the Western Army section (E/320 and Penguin) had something of a S.S. flavour. There was in addition the class of Police keys which deserves separate treatment.

[K] Also in most cases the corresponding reserve keys - some of which were used.

Police Keys The German Police was characteristically much more closely related to the Army than we should think fitting: in particular, it was closely bound up with the S.S. and high functionaries often held rank in both services. But for most of the war the Police as such had no machine ciphers$^{\Theta}$: they made do with hand systems such as Double Playfair which were successfully dealt with in another section of Bletchley Park. It thus happened that when in February 1944 the Germans at last decided to introduce an Enigma key for the higher police officials in occupied Europe there followed a close collaboration between two different cryptographic sections to break this key named Roulette (Polchi M/S). This kind of collaboration was not of course unique in the history of Hut 6; but there were few, if any, keys on which we were so dependent on outside aid for breaking as in the case of Roulette.

The introduction of Roulette did not result in the disappearance of Double Playfair which in fact remained the vehicle for most of the Police traffic; and the first breaks of Roulette (February 10 and 16, 1944) were made on R.E.'s from Double Playfair. (Throughout the whole history of Roulette indeed most breaks were made on R.E.'s - probably not far short of 45 days out of a total of about 60.) These initial breaks showed that Roulette followed almost universally the Double Playfair practice of burying addresses in the middle of the message. Even had this not been done it is unlikely that the very varied addresses and signatures would have proved cribbable: but the universal burying made it impossible even to consider attempts.

Roulette is a standing example of how easily the Germans could have defeated cribbery by sufficiently thorough measures: the burying of addresses and signatures in the middle of the message is an even more effective measure than the alternative system of wahlworts which they did eventually use very extensively on the Army and to a slighter extent on the G.A.F. It has indeed only one serious weakness: if there is in the traffic a routine Tagesmeldung, Lagebericht or the like by burying the address one may actually make the message a better crib as it then starts with the Tagesmeldung part. For a short time in fact Roulette had quite a good crib of this nature, the "Routag" (a report on anti-partisan activities in Albania) that flourished in the last week of March and the first week of April. But this crib had a short life and its successors were still more ephermeral. Roulette in fact largely escaped the danger mentioned above for two reasons: (a) there were in fact no routine messages that lasted for any length of time and (b) those routine messages that did occasionally turn up and were sometimes spotted on evidence of past police decodes were largely spoilt as cribs by the odd contractions they might use e.g. TAGESMX VX for TAGESMELDUNG VOM. It may be remarked that Roulette was notorious (even among keys of its class) for the frequency and strangeness of its abbreviations - for instance, any word ending in DUNG could be contracted to DGX.

A few Roulette days were broken on psillies or cillies and these entertaining stories are worth recording. On April 6, for instance, we had two messages with the following sequence of outside indicators WIR,UCH, IGA, TEN and the same message settings: the blanks were filled up thus: WIR-BRA UCH-ENZ IGA-RET TEN (= We want cigarettes) and the day was broken on this missing word competition. Again on July 11 the day was broken on cillies from DRT (Laibach) and the full list of settings used is worth

$^{\Theta}$ Perhaps one should except the Secret Police (Gestapo). It is generally considered that T.G.D. was in a sense their key. Roulette was the key of the Regular Police (Ordnungspolizei or Orpo).

mentioning - WIG^{5}, SPI^{3}, PAU^{3}, PAM ^{2}, HOE^{2}, HER, HOH, HAH - while a few days later a key was broken on WIG^{3} plus BETRX.* However, these cilli stories were exceptions and the CY system (which was introduced on Roulette somewhat earlier than generally - viz. at the beginning of September) effectively ruled out the possibility of cillies.

So with few exceptions Roulette was broken on R.E.'s. Of these the supply was fluctuating and not all succeeded: the success attained was probably about 60%. In August 1944 the supply of R.E.'s reached its peak and no fewer than twelve days were broken during the month. But in September this supply suddenly dried up owing to the replacement of Double Playfair by a much superior hand system known as Rasterschlüssel. This led to an awkward situation: for much the best means of breaking Roulette was on Police R.E.'s but with this new system in force Hut 6 was now asked to break Roulette on its own in order to give R.E.'s into Raster.

We promised to do our best but the situation was very difficult. We had kept full records of anything that looked like the shadow of a crib but when all this material was put together in order it was hardly possible for the most optimistic cryptographer to feel confident of success. Besides any attempt would be most expensive in bombe-time: and there were severe limits to the time we could spend on Roulette even when full allowance was made for the increased cryptographic importance of Roulette as a lead into Raster.

Our utmost efforts were not entirely useless: for we succeeded in breaking Roulette of October 7 on a vast stagger job and this break was a distinct help to the Raster party. But it must be admitted that in the main the Raster cryptographers had to fight their own battle and indeed we had from the beginning of the crisis warned them that salvation could only come from their own efforts. In the end the Raster system was largely mastered and the supply of R.E.'s started again, though never quite on the same scale as before. The course of the crisis is well mirrored in the monthly figures of Roulette breaks:-

August	1944	-	12
Sept.	"	-	2
Oct.	"	-	1
Nov.	"	-	0
Dec.	"	-	7
Jan.	1945	-	2
Feb.	"	-	2
March	"	-	3
April	"	-	6

These breaks were mostly effected on the old R.E. lines but it is worth noting that the last breaks in April 1945 were partly due to a few tolerably indifferent cribs of which the most amusing was the so-called "Letter to Rauter", a short report from the notorious Seyss-Inquart to Frau Rauter, wife of a high police official in Holland. Incidentally, these messages often appeared to us to be written in an absurdly optimistic vein.

Roulette was in general broken late: this was because we were so dependent on the R.E.'s which in turn - especially in Raster days - were broken far from currently. So more often than

* The indices denote the number of times the message setting occurred - of course not all were cillied.

not we were running about a month behind on breaks: and thus it is not surprising that some of the last breaks scored by Hut 6 were of this key - no fewer than four April breaks were actually chalked up after VE Day.

It should be stated to conclude this account that to begin with Roulette had certain peculiarities (such as the discriminant in the first group and the use of only one wheelorder per day) that were oldfashioned by the standards of other keys. But in April 1944 Roulette began putting discriminants in the preamble while by December it was using three wheelorders per day. This brought it into line with other keys except that all Roulette messages discriminated.

In the matter of routeing Roulette was treated differently from any other Hut 6 key. The traffic came to the Police Section, was there blisted and afterwards brought down to Hut 6 for examination. The decodes in their turn went back to the Police Section, not to Hut 3, as was the case with other keys.

The discovery of R.E.'s between Police ciphers and Roulette was not done by Hut 6. These were reported by our colleagues in Lt. Col. Evans' section and were often in fact first noticed by the Police log readers. Our task was confined to working the R.E.'s that were discovered. In other respects also the Police Section helped us e.g. by looking for any routines known on their keys. It is thus obvious that Roulette cryptography (to a greater degree than any other key) was only partially in the hands of Hut 6 and we must unreservedly acknowledge the great assistance we received throughout from our Police colleagues: it was unfortunate that owing to the highly intractable nature of Roulette in its own right we remained to the end so dependent on a lead from them.

It only remains to add that a few minor Roulette keys appeared from time to time: the so-called Roulette II which used the Red key and had useful cribs; Roulette III dealing with electricity supplies in the Ruhr and only once broken; and Roulette IV which was really Quail used sporadically by a few police stations in the Balkans. Of these only Roulette II had any cryptographic importance.

1·8134 Summary

The exploitation of the S.S. and Police keys can definitely be said to have been cryptographically successful: the most important key, Quince, was broken almost daily for long periods on end and every key that passed any quantity of traffic was broken frequently with the exception of T.G.D. With respect to this last failure it must be remembered that pressure of other commitments made it impossible to maintain adequate and continuous cover on T.G.D., so it was never subjected to a concentrated and long-sustained cryptographic assault; but honesty compels the admission that the key always seemed so unpromising that no one can say whether even a full-scale attack would have succeeded. But apart from T.G.D. there were no serious failures in our attack on the S.S. keys. On the whole the success attained was satisfactory in view of the intelligence rating of the colours[¥] - any increased success could only have been secured, if at all, at the expense of more important and urgent commitments.

¥ It must be remembered that the S.S. keys were never operational. Their importance did tend to increase towards the end of the war but even Quince I or Quince II - the best keys for intelligence - were never considered better than good second-class keys at their peak - though it must be remembered that this was a respectable rating, as five or six classes were recognised.

1·814 MUSTARD

1·8140 Introduction

Mustard was one of the last keys to be named before the rigid application of class distinction was made and the name arose by natural association with Mr. Colman, the head of the Control Room. Whether the namers had also in mind the arguments about mustard in "Alice in Wonderland" or whether the name was merely happy foresight, the fact remains that the Mustard organisation in the first instance at least had no links with other G.A.F. units and so would have been difficult to classify under the headings adopted.

The Horchmaschinenschlüssel or key of the G.A.F. Y Service first appeared in June 1941 on the invasion of Russia and was used by those Signals units with Y duties for sending intelligence reports on Russian wireless activity back to centres where these reports could be collated, codes broken and the intelligence issued to interested parties. As active fronts appeared in the Mediterranean and the West, so did Mustard networks and keys. Behind each front there was usually one main centre to which all information, reports and D/F's were sent; these centres at Warsaw, Rome, Athens and Paris forwarded, when necessary, items of interest to the head office in Berlin.

Mustard provided the first example of one key being used with four sets of discriminants - a device presumably adopted to camouflage the use of one key over a wide area. This meant that, for security reasons here, Mustard was divided into I and IV on the Eastern Front, II in the Mediterranean and III in the Balkans. The Mustard networks in the West did not become active until after D Day when the other Mustards had been reduced to Mustard II, covering Italy and the Balkans. Western G.A.F. Y messages were sent in an assortment of keys including Jaguar and Red, but Mustard I and Cress were the normal keys.

Each Mustard in turn was responsible for the breaks recorded; for Russian Mustard was the source of practically all breaks until 1943 when the Mediterranean Y services took over the task of keeping us informed of what the Germans knew about the Allies.

1·8141 Russian Mustard : Mustard I, IV

The initial break into Mustard was made in June 1941 on cillies, and keyboard cillies (favourites were PAQ, PAP, QAP) supplemented by the beginner ANX WX EINSNULL (W10 was the cover name for the Warsaw office) accounted for most of the twelve other breaks in August and September. The strength of the few cribs shown by the evidence of these broken days can be judged by the fact that no break was effected on them after the cillier had gone. Indeed, the rest of the year was a blank and this unhappy state of affairs continued until April 9, 1942 was broken on pronounceable cillies. Even here there was a disappointment; for, while some of the Mediterranean Mustard decoded, one frequency, 9840, remained obstinately dud. But this was to be the last misfortune for a year as a few days later the first of the quadrilateral key repeats was discovered and for the rest of the year Mustard was involved in these repeats. March Mustard keys were known when both April Red and Foxglove were out, and could generally be broken if only one of the components was known. Moreover, once the significance of a discriminant repeat had been established, it was possible to delve into the unblisted masses

of January Mustard and rod out a day on the stecker of February Red. When it was found that January Mustard had the wheelorder and ringstellung of February Primrose, most of the January days only needed blisting and decoding. Incidentally one reason why Mustard was not infrequently a victim of pressure of work in R.R.2 was that at this time the traffic consisted of long messages (up to 60 teile a message) giving the Russian Order of Battle and other information intercepted. As these messages could be subtracted on the register, there was not the same urgency for blisting as on other keys.

Fortunately the key repeats in 1942 coincided with an outburst of cillying on these long messages and the combination of these two factors often made breaking an academic exercise. In June, the operator at Shitomir realised that the whole business of encoding and decoding might be enlivened by the use as message settings of sentences chopped up into three-letter groups. So, appropriately enough, he started on June 15th with the cilli sequence WIR/LIE/GEN/INX/SHI/TOM/IRX which was the first time intelligence had been derived from message settings. The idea was taken up by other operators and greetings and good wishes were popular, especially at Christmas time. Apart from sentences, such a cilli sequence as ANF/MIT/MUT/GOT/END (used in January 1943) was very typical; ANF and END were particular favourites. A more unusual sequence for a German operator - OLD/BOY/HOW/ARE/YOU - was used more than once in the year of cillies and repeats, and indicator habits in general became so well-known that it was possible sometimes to make correct guesses at message settings even when the operator had attempted to disguise his favourites by twiddling three or four on every wheel. With the large number of breaks cribs were established which helped to fill in cillibss days. After the end of the great period of key repeats in December 1942, Mustard was still broken regularly for some time, naturally not so often as before, but as frequently as was necessary for the intelligence sections to keep their Russian Order of Battle up to date. However, the introduction of wahlworts in February 1943 was speedily followed by the decay of Russian Mustard and although thereafter some long messages did appear and even cillied once or twice, the cryptographic centre of Mustard moved permanently to the Mediterranean area.

1·8142 Mediterranean Mustard: Mustard II, III

Although the story of this region does not really start until the cryptographers were forced to scratch around for cribs after the end of the Russian cillies and cribs, there is a prologue in the shape of 9840 Mustard left dud in the last section. With the recent precedent of Orange 4152 it was only natural that attempts should be made to rod out 9840 Mustard. There were no cribs but various beginners were tried without success; finally in a mood of considerable scepticism a Test Plate job was prepared and produced on one message the beginner ANX WILLIX EINSNULL. Then it was discovered that every message on the frequency had a <u>different</u> ringstellung which was determined by a daily changing figure code on the last three figures of the G.T.O. while the key otherwise was ordinary Mustard. Thus e.g. on March 10, 1942 the code was

1	2	3	4	5	6	7	8	9	0
B	T	K	P	C	G	J	E	U	M

so a message at 1943 had German ringstellung UPK. It was necessary first to break the normal Mustard key and then to rod a number of 9840 messages until the full substitution for the day

had been discovered. This device only lasted for a month or two and was then abandoned, presumably as being too much nuisance from the German standpoint.

When, however, the decline of Russian Mustard turned our attention anew to the Mediterranean Mustard, useful cribs were discovered; and, though all used wahlworts, these were generally limited to from four to six letters. The cribs at this time all originated from Crete, the best being Jagdflugtätigkeit and the others the long-lived Einsatz Eins and Einsatz Drei, all of which were named from their initial words. The first of these disappeared in July and for some time after that the breaking of Mustard was less frequent and more expensive as the other cribs were shorter and subject to occasional irregularities of form. Mustard certainly suffered also by its expense in bombe hours and its comparatively low intelligence rating.

By September 1943 the position had become so bad that not even the unexpected evidence of a week's Mediterranean Mustard traffic on Red (due to a capture of Mustard keys by the Italians) helped us to continue breaking and the ephemeral reappearance of cillies on Russian Mustard gave us a couple of days in October and one in November without influencing the long-term prospects appreciably. But in December 1943 a new type of traffic appeared on Mustard which led to a remarkable improvement in the situation.

On December 14, 1943 a string of short KR messages appeared on the Balkan Mustard and, as these messages cillied to keyboards, the day was soon broken. These messages continued to appear on other days in December and January and continued to cilli to keyboards or pronounceables; and with the knowledge of the message contents it was possible to use them as cribs and sometimes to read them in depth as the message settings were known. It was discovered that the messages were "H" reports originating from Durazzo giving details of our air penetrations into enemy territory and there might be any number from 8 to 60 a day. They consisted of a reference number and a string of code names which changed monthly but could, in general, be predicted with fair accuracy. A report on Mustard published in January 1944 gives as a current example of a typical "H" message H X VIER X MUMIE X PIRAT X JU WEL X LEUTE X PRIMA X PEDAL X INDER X HEQT where the predictable code names are underlined. As a good example of the possibilities of depth reading we may cite January 8, when two messages cillied to PAT and PAR and fitted thus:

```
R Y X V - - F S M S K X F
H X E I N S X F R A N Z X

P M Y M E X F C F S M S K X F
Z U X H X Z W O X F R A N Z X
```

Of course such gifts from the gods did not last for long; but the current crib situation on Mustard was clarified. The Einsatz cribs were still to the fore in somewhat changed guise. In our notation, there was the Einsatz Mark I, sent from Athens to Belgrade three times a day, about 0500, 1400 and 1800. Early in 1944 the wahlworts used were exclusively three to six letters long and at the appropriate hours of day it was better than an even money chance that they would be GUTEN ..... MORGEN and GUTEN ..... ABEND. In January 1944, the wahlwort GUTEN was used successfully - for the first but not the last time - to eke out the otherwise short crib.

With the Einsatz cribs and a few inferior second strings Mustard was broken happily and regularly throughout the summer of 1944 - in fact from June 8 to July 15 there were only two missing days. Latterly much of the damage was done by the Einsatz Mark II, a crib sent out several times a day from Durazzo. In January this crib which had a long variable address is described as "dingy" but it improved considerably from April onwards and eventually supplanted the Einsatz Mark I as the standard means of breaking Mustard.

After August 1944 there were fears that the Mustard position might be ruined by the spread of Reflector D; it was not, however, until October that Mustard used D and our breaking was hardly affected as the Balkan Mustard remained on B. In November, however, there was a sharp deterioration in the crib position due mainly to the confused Balkan situation: and on December 1 Mustard split at last into two keys, Mustard I for the West (on D and unbreakable), and Mustard II for the South, the Italian stations using D and the Balkan stations B. Several breaks of Mustard II were made in the first half of December but the veteran cribs were now on their last legs; and in fact December 15, 1944 was the last Mustard of any kind to be broken in Hut 6.

1·8143 Western Mustard and Cress

A brief note should be added about Mustard in the West. Until after D Day there was very little Western Mustard: just after it there was for some time a good deal but it came out until December on the same key as Mediterranean Mustard, so we were relieved of the hopeless task of trying to break it in its own right. Indeed for some time after D Day Mustard became to some extent of operational importance, as the Western Mustard was giving R.E.'s to Jaguar, one of the principal G.A.F. Western keys.

A second Y Air key that appeared in the West, Cress, was also much mixed up with Jaguar, and was broken several times on cribs that had migrated from Jaguar or on R.E.'s. We can never, however, be said to have got a firm hold of this minor key.

1·8144 The End of the Story

Little indeed can be said of Mustard in the last months of the war: increasing preoccupations with more important keys and the general problem of encoded callsigns had driven it more and more into the background and the last reference in the Hut 6 weekly reports in January 1945 merely notes that it is in a very poor way. So far indeed had Mustard become a wraith of its former self that it hardly needed the last blow of encoded callsigns to banish it to oblivion - if indeed that word can ever be fittingly applied to a key that throughout its history did so much to enhance the gaiety of Hut 6.

1.815 T H E V - K E Y S

1.8150 General Introduction

Compared with the themes of other chapters, the present subject is very restricted and well-defined. It is concerned with three keys only - Corncrake, Ibis, Jerboa - which all flourished within the period March 1944 to the end of the war and were all concerned to a greater or less extent with the V1 and V2 weapons and the attacks on this country. Jerboa, an Air Key, was concerned with V1 attacks; Corncrake and Ibis with V2. The difference was that Corncrake dealt with the experimental and preparatory side while Ibis appeared in the period of rocket attacks and referred to the actual operations.

It seems convenient to treat these three keys within the same section but they will be discussed in separate sub-sections. This can be the more easily done because there is no real geographic or cryptographic connection as has been the case with most groups of keys previously discussed; Corncrake, Ibis and Jerboa have no point in common beyond the general subject with which they dealt. The keys are indeed not a regional or cryptographic but an intelligence unity - as such they were dealt with by the same section in Hut 3.

In Hut 6 the keys were all treated on a Research basis - no attempt was made to break them currently by the Watch. Neither their intelligence importance nor their cryptographic stability demanded or justified such an attempt. Corncrake was dealt with by Army Research and Jerboa by Air Research; Ibis which only came into being after the abolition of Research was a key of the Army Qwatch.

One other point should be mentioned before we discuss the keys in turn. The grouping of these three keys as V-keys should not allow us to forget that there were other keys that give valuable information about V-weapons. Brown in particular gave over a long period hints on the developments of V1; and other keys such as Lily, Orange, Falcon gave more occasionally useful sidelights on these topics. But in the latter case the information was usually given incidentally in keys mainly concerned with other matters; while Brown(which in any case is fully dealt with in a separate section)covers the whole period of the war, not merely what we may call the "V-period". So now that due acknowledgment has been made of the contribution of these other keys we can still with a clear conscience style Corncrake, Ibis and Jerboa the V-keys par excellence.

1.8151 Corncrake

The history of the breaking of Corncrake is so brief and yet so full of interesting points while it lasted that it is both possible and desirable to treat it in rather more detail than can generally be done in this history. In most cases our important colours were relatively long-lived and breaking extended over a period of many months or even years: in the case of Corncrake the breaking period is from the middle of May 1944 to the end of July.

The story really began about the middle of May 1944 when in accordance with what was then established practice a long message - actually a 7-tle - was brought in to Army Research K by a member of the T.I.S. for routine examination for cillies. This was a standard precaution specially intended for new and obscure groups so that no chance of a snap break should be missed and ninety nine times out of a

K This then contained all the Army cryptographers. The Army Watch was not set up till D Day and the Watch was at this moment wholly concerned with Air keys.

hundred nothing came of it: the message was tossed aside after a hasty inspection. But this was the hundredth time. The delighted cryptographer discovered the cilli sequence FRI, FRA, FRE, FRO, FRU - settings that were amply confirmed by counts - and the day was quickly out on a bombe menu.

This initial break - E/6245 of May 13 - was a virtually unknown group: we had no reason to suspect it was of any unusual importance and the break was effected simply in the normal line of business. The motto of Hut 6 was to break everything possible whether it was considered important or not - a principle whose ultimate validity even on intelligence grounds was proved again and again; perhaps never more so than in the case of Corncrake (as E/6245 was soon named).

The contents of Corncrake created an intelligence sensation in Hut 3: the exact significance of much of it was obscure but it clearly referred to scientific artillery experiments of importance and was described as an "Army equivalent of Brown III". Strong representations were made from the highest quarters in the Park in favour of a determined drive to break more days and the work was at once set under foot, the new key being assigned to a parent as was our usual practice.

Enquiry from SIXTA - who were always referred to on the emergence of new and obscure groups - showed that Corncrake had been known as a W/T group since December 1943 but could not be said to have passed traffic in any quantity at all till March 1944, and even in the early part of March traffic was very low. Signs of cillying had been noticed from time to time and in fact one or two days had been run unsuccessfully before the break-through in May. As often happens in such cases one break was quickly followed by another - the 19th April came out on cillies plus STRIQ VIER VIER GEHEIM(which had appeared on May 13th).

The W/T system of Corncrake was simple. There were three stations - Heidelager, which acted as control, Peenemunde and Koeslin - all distinguishable by the rows of their callsigns. Practically all the traffic was to or from Heidelager, i.e. the messages fell by routeing into four classes under which the traffic was entered. The original couple of breaks, however, revealed nothing that could be regarded as a crib [1] and the possibilities of "cilli plus" menus were soon exhausted. So as a last resort we decided to run the Secret Tail - STRIQ VIER VIER GEHEIM - on all promising messages. This was a recognised line of attack on Army keys in general: in the case of Corncrake it was known to occur sometimes, it was also known to be very bad, but it was still considered worth running on the grounds that a large number of shots might break one or two days and so get us going. This is a line of attack that can only be practised with considerable reserves of bombe power such as we had in 1944.

[1] A small compact system is unfavourable to the rise of cribs - e.g. Brown for most of its life. Brown's good crib period was when it was fully operational.

The Secret Tell drive proved successful after a blank week: out of approximately two dozen days run two May days came out X. On this further evidence two more days were broken on cillies plus an address AN VERSUQSKAB. It was only at this stage, i.e. when some half-dozen days had been broken, that what was to prove the best line of attack appeared. It was discovered that a number of messages to Koeslin started off with the "Wagnerian Address" AN KO STELLE SIEGFRIED and this broke three days in the week ending June 10th and no fewer than eight days in the following week.

We had now secured a good entry into Cornrake and exploitation went forward rapidly. From the nature of the key back days were as valuable as current breaks and the traffic back to March(prior to which it was all too scrappy) was examined and produced on concurrently with the new traffic that came in. In all 33 Cornrake days were broken [1] of which precisely two-thirds were on various forms of the Wagnerian Address and most of the rest were on cillies plus. A couple of days were even broken on a sporadic crib - a numbered BESTANDSMELDUNG which must have been sent out daily but was rarely passed on the air. It will thus be seen that Cornrake provided in a peculiarly pointed form an illustration of the fact that the best means of exploiting a key are not always obvious until quite a number of days have been broken on inferior and laborious methods.

Cornrake met a sudden end with the evacuation of Heidelager on July 23rd and no traffic was passed after this date. Possibly this quick death was preferable to the slow decline of other keys. It is true indeed that in September a key was captured (Soldor Maschinenschlüssel F-W Kão II) which decoded traffic on a couple of days that was Cornrake in content. But it proved impossible to break this revived Cornrake and traffic swiftly declined to the lowest levels. The friends of Cornrake will prefer to forget this ineffectual ghost and to date the funeral obsequies of the true bird to the fateful 23rd July.

1.8152 Ibis

The history of the breaking of Ibis is even more highly concentrated than in the case of Cornrake. Apart from one belated success all the breaks occurred in a period of about six weeks from February 12 to March 24, 1945.

The traffic was, however, being examined for a considerable period before the initial break was secured. Ibis traffic was in fact passed in small quantities as early as October 1944(it will be remembered that the rocket attacks on London began in September) but it was not at first recognised as a separate group and was blamed along with other miscellaneous scraps on a section of the composite Western Front blist. In November, however, the seperate identity of Ibis became clear and the key was named and blisted seperately.

[1] Later evidence showed that this was just about the percentage of success we were entitled to expect.

[2] The figures were March, 2: April, 5: May, 11: June, 10: July, 5.

From the W/T standpoint, Ibis (or the Z2 complex in the SIXTA technical nomenclature) was a somewhat complicated study. At various times no fewer than ten stars were recognised which passed not only Enigma but quite large quantities of traffic in other ciphers [C]; and in fact one method of identifying the Enigma traffic as Ibis was the appearance of the stations concerned passing these other ciphers, some at least of which were readily identifiable at sight. It was soon suspected - mainly by coincidences of messages with times of rockets - that the non-Enigma traffic at least in the Ibis system was concerned with the launching of rockets and this was eventually confirmed by breaks. This traffic, known as VEGA, was dealt with by Major Owen's Section(then in Block F).

As soon as it was established early in December that in all probability Ibis dealt with the V2 attacks it was recognised that it was highly desirable and might be most important to break the traffic. In complete contrast to the case of Corncrake, Ibis was now attacked in full knowledge of its nature. But while this knowledge gave the cryptographer an added incentive to break the traffic, it did not give him the means to do so: cillying was non-existent, R.E.'s could not be expected, and while certain possible routine messages did appear too little was known in detail of the units and personnel involved to make anything like cribbery possible. We seemed indeed to be up against a blank wall: and in sheer desperation after the failure of several G-tails and the like a mammoth 63-versional stagger was produced on a January day - the stagger being the number of a unit which it was thought might appear in a message. Fortunately it was not necessary to run this drive through to the end, as on later evidence it would certainly have failed.

But when the outlook was at its blackest light shone out of the darkness. Towards the end of January we received information that a part of the VEGA system had used Double Playfair that month, and that a number of days - eventually nine or ten - had been broken. Examination of these decodes revealed that they were all on Star 0 and consisted of messages to and from the launching batteries in Holland. What was still more important the batteries were in the habit of each sending in an evening message to the control of the group a list of the rocket launchings and some of these reports appeared cribbable. Finally it was clear from the traffic on Ibis that while in January these reports(for some reason unknown to us) had passed on Double Playfair E, in November - December 1944 and February 1945 they had passed and were passing on Enigma.

Immediately a campaign was opened on these reports - Rocket Bradshaws as they were called - and on the 12th February success was attained by the breaking of 4th February on one of these messages. This success was soon followed by others and by the beginning of March seventeen days had been broken on the Bradshaw, three February days and the rest December 1944. The reason for this preponderance of December days is rooted in the nature of the crib.

[C] Actually only three stars - 2, 4 and 8 - ever passed Enigma in any quantity.

[E] Because of this there was very little January Ibis and as the cribs to be now described were absent, January Ibis was never broken and in fact not much tried.

The title "Rocket Bradshaw" must not be regarded as the name for a specific message, like most crib titles. It is rather a generic title for a group of messages from different stations and in many diverse forms and agreeing only in their general content, viz. that they all gave times for the departure of rockets from Holland; the times of arrival in England - four minutes later - were not given. These messages generally began with a "framework" which was followed by the times in correct sequence. How some of the stations involved varied the framework considerably but one particular station was most consistent in using the form START AM day x month (x) UM time, and most days were broken on this. ¶ The station in question was far more active in December than in February and this was the principal cause for the larger number of December breaks.

It was possible to obtain from Major Owen's section the times of rocket launchings as given by the various batteries in their low-grade ciphers, and in fact this information was passed on to us regularly. As these times ought in theory to be - and often were in practice - the same as those enciphered in the Rocket Bradshaw messages, it might have been thought that at least sometimes the whole message could be written out as an R.E.: but for various reasons this was impossible. First, the times as given to us were not always precisely the same as in Enigma (this was apparently due to corruptions in the low-grade ciphers); and secondly, it was in practice impossible to make allowances for such parenthetic remarks in the fate of a particular rocket (e.g. "faulty start", "bursts where it stood" and similar misadventures) as did occur in Enigma but were normally absent in the other ciphers. The first time of launch, however, was quite often used to eke out what would have been an insufficient menu: the hour (which was pretty safe) was generally all that was employed. Also towards the end of February and the beginning of March when what we have called the framework of the Bradshaw had become uncribbable from the variety of forms, we tried the experiment of running the Time at End, i.e. trying the last time given to us at the end of the message. This usually failed, but did succeed in breaking three days - and every day counted on this and indeed the V-keys generally. It was, however, sometimes possible on "nil return" days to write out the whole Rocket Bradshaw and several days were broken on

AM FUENF X EINS ZWO KEIN START

and the like. There were also several examples of a 14-letter message saying

HEUTE KEIN START
or KEIN START HEUTE

but on unbroken days this as a rule gave us the cryptographer's hoodoo - a certain crib that is too short to run.

The breaking of one particular Feb's day, February 1st, is worth recalling. For the first four days of the month some of the traffic was in a curious "code" which was in fact little more than a kind of shorthand. The message consisted mainly of a string of numbers represented by their first letters (or in a few cases a later letter when the initial letter would have led to ambiguity) i.e. L = 0, E = 1,

¶ Of course the original evidence for forms used was the Playfair messages for January. The assumption was made that these would be the same as the Enigma forms in December and February: fortunately this proved to be correct.

Z = 2, D = 3, V = 4, F = 5, S = 6, I = 7, A = 8, N = 9, with X, Y and T as punctuation. It was possible on the evidence of the 2nd to the 4th to build up a rather stereotyped framework which was true for at any rate a fair number of messages and this curious crib "XY" was run on two messages on the 1st and broke the day at the second attempt. The "crib" ran something like this:- 2

FL.....X.Y..X.T..X.Y..X.T..X.Y..X.T..X.Y..X.T..X.Y..X.XY.SD..X.

By 24th March, 22 Ibis days had been broken, 15 being in December ⅔, 6 in February and 1 in March. But the course of Ibis was now almost run. Traffic which had reached its flood at the beginning of February with 80 messages a day had declined to a trickle in March and vanished altogether in the last week of that month - a development not unconnected with the German collapse in the West and the consequent discontinuance of the rocket attacks. It was thus possible to write at the end of March; "To Ibis we hope to have bidden farewell".

Yet this was not quite the end. From the nature of the traffic, the date of Ibis decodes was largely immaterial and in fact some of the best intelligence came from the December breaks. It was now admitted that the period December to March had been cryptographically exhausted; but little had been run on earlier days and during April Hut 6 was approached by the intelligence experts of Hut 3 with the request for a drive on those early days. An investigation was accordingly made and it was at once apparent that nothing could be done with the scraps of traffic in October; but November seemed to offer some possibilities and contact was made anew with Major Owen's section to secure the necessary information of continuity of callsigns and rocket launching times ⅝. A drive was prepared on the best days and sent to the American bombes - which throughout did invaluable work on Ibis. Honour was satisfied by the break of one day, November 28, on May 8, 1945. Symbolically at least it was not unfitting that the final break of a V-key should be effected on V-day!

θ Unusual as this was, it was not quite unprecedented; "Code Cribs" were not unknown on Blue and Brown.

⅔ For peculiarities of December keys see the final section on Rules of Keys.

⅝ It will have been noted that in the case of Ibis(as in that of Roulette) we were greatly indebted to external assistance in the preparation of material to run. On Ibis our dependence was not on the whole so great though it must be admitted that the initial break would never have been secured without the crib evidence supplied by the work of Major Owen's section.

1.8153 Jerboa

The history of breaking Jerboa has analogies to both of the preceding stories. Like Ibis, Jerboa yielded all its breaks-20 days in all - in a very short period, less than three weeks from August 13 to September 2, 1944. Like Ibis, again, Jerboa was only broken at all on evidence supplied by breaking a low-grade cipher; while like Corncrake it had a second birth which was a sad anticlimax to its great days.

Jerboa first attracted notice as an Air group in Western Europe in July 1944 and a few G-tails were run. It was known from 3-letter traffic(known as KLAVIER) passed by the same systems that it was connected with the launching of flying bombes but for some weeks there was no good line of attack. Eventually, however, an early morning routine message appeared which was thought on KLAVIER evidence to give the time of the next tuning message. We had had experience of this type of message on various Air keys and knew roughly the sort of forms to try, and on August 13th July 26th Jerboa came out on the beginning DER NAEQSTE ABSTIMMSPRUQ WIRD AM. In the following weeks this form broke many other days and several other forms were discovered by trial and error. To the end we were never able to claim that we could break any day - the Spruq did not reveal all its twists and turns - but the final result of a swift campaign was that 20 days in July and August were broken on the Spruq and September 1st on a stray R.E.from Jaguar. Traffic was always very low, sometimes, indeed consisting of the orib message only.

Early in September Jerboa disappeared in consequence of the Allied advance through Belgium and France. Its absence was hardly regretted as the Spruq, the only means of breaking, had disappeared a few days earlier. By October even the name Jerboa had disappeared from our traffic statistics.

In December again and in February - March 1945 there was a recrudescence of Jerboa traffic which reached its peak in the week ending February 24 with an average of 51 messages per day. In the next week this fell to 15 and then vanished for ever. It was quite impossible to find any entry into this revived Jerboa; the only ray of hope discovered was that there was some reason to believe that March Jerboa might be using Indigo, the G.A.F. teleprinter key. But this proved a will-o'-the-wisp: the Indigo key was captured and did not work.

1.8154 Importance of the V-Keys

It was not in general the business of Hut 6 to form opinions on the relative intelligence importance of various keys. While, of course, in decisions of bombe policy regard had to be paid to the intelligence rating of keys we had recourse to the gradings periodically published by 3L. In accordance with this limitation of Hut 6's responsibility the present history does not normally discuss in any detail the intelligence value of keys. But in the special case of the V-keys their importance was of such a peculiar and unusual nature that it seems justifiable to pass beyond our usual limits and discuss the matter briefly in general terms.

It would hardly be untrue to say that in their own way the V-keys were among the most important broken in Hut 6;but such a statement would be open to serious misapprehensions unless the

nature of their importance was understood. The importance of other keys lay in the degree of their relevance to operations that were already in progress or impending; in general the most important and urgent keys(as e.g. Ocelot and Jaguar among Air keys; Bantam and Puffin among Army keys) were those that were immediately and tactically concerned with current operations or strategically relevant to the conduct of future operations. The V-keys had none of this kind of importance, not even in the case of Ibis, which gave the times of rocket launches. This was because their reports were historical - so that even if the key could have been broken currently the decoding of these messages would only have told us what rockets had been launched against England - a fact presumably already known. (Had the reports been of intentions to launch rockets at future times the case might well have been different.) For this reason there was no special advantage in current breaking.

The breaking of V-keys was thus not of immediate operational significance; nor was it on the whole(once the attacks had started) of significance so far as counter-measures were concerned. The problem of defence against V1 had to be, and was, worked out in the practical field of action: the contributions of our intelligence to this lay in forecasting the probable scale and manner of the attacks before they took place. Against V2 there was from the nature of the weapon no effective defence (apart, of course, from the clearance of the rocket sites). The true significance of the V-keys lay in a longer issue - in their general relevance to the future of warfare.

It may truly be said that in the last year of the war the Germans were endeavouring - with such measure of success as the increasing pressure of the Allies permitted - to change over from one type of war to another. It has doubtless been true from the beginning that this has been the most scientific war in history: but it is clear that the Germans towards the end were finding their way to a kind of war that would be scientific in a still fuller sense - a type of war in which the scientist and the weapons he invents and develops will be the decisive factor and no longer generals and admirals, armies and fleets. It may be claimed indeed that in their obsession with this new type of war - an obsession fully proved not only by the V-weapons they used but even more so by those they planned= the Germans lost their sense of reality, that in reaching out after the future they sacrified the present: but however that may be no one can doubt that the V1 and the V2(to mention nothing more) are true forerunners of the weapons of a new war.

If it is admitted that the achievements and visions of the Germans in this last phase foreshadow the future lines of advance of the art of war, then the true significance of the V-keys becomes apparent. It is obviously essential for our present and future research that we should know in as precise detail as possible exactly what the Germans have accomplished in these highly technical fields. Now that the war is over we have other means - e.g. interrogation of prisoners - available to discover the exact position reached by German practice and theory; but before the war ended the V-keys represented the best means of obtaining the necessary insight into German scientific progress. This is especially true of Cornrake which dealt with these matters on a higher level than the other keys.

This peculiarly long-term importance explains how date and currency were largely irrelevant: there was a certain timelessness in the scientific content of much of these keys. Also the matter

was so technical that it was desirable to break as many days(of whatever date) as possible as any new break might explain hitherto hopeless obscurities in a day already broken. Old days were at times indeed specially desired so that one might catch the beginning of some scientific argument. The difference between the importance of the V-keys and other keys broken by Hut 6 is illustrated by the fact that for most keys priority of decoding ran in backward order of date while for the V-keys the converse was true.

To sum up in a sentence - while the importance of most Hut 6 keys was in the degree of their immediate relevance to current military operations the ultimate significance of the V-keys lay in their long-term connection with the probable future of developments of science as applied to war. ¥

¥ To avoid any misapprehensions of the writer's position it should be stated that the above is not meant to convey any fatalistic acceptance of the inevitability of future wars. It merely involves what must surely be considered a justified conclusion about the nature of future wars(if these arise) and a belief that until the very possibility of future conflict is excluded for ever common prudence for the safety of our country demands that we take steps to ensure that our science is not behindhand in these technical developments - which in turn underlines the necessity for full knowledge about the scientific progress of our enemies.

1·816 FIRST BREAKS OF KEYS

It seems fitting to conclude the series of key histories with a chronological list of the first breaks of every key that was given an individual key name. This will give a picture of the constant expansion of the field of our breaking: for instance, up to the end of 1940 we had broken 8 different keys, by the end of 1941 the figure was 25, and in the subsequent years it rose to 61, 108, 170 and finally 181.

It will be realised that a number of difficult points have arisen in compiling this list and it has seemed best for the sake of consistency to adhere rigidly to certain rules.

(1) Dates The date given is that of the key broken, not the date when the break was effected -- this was usually later, sometimes much later. Also it is not necessarily the first day we broke of the key in question, but the earliest date among the full tale of broken days. Probably in most cases one would get the same answer, but on keys like Corncrake and Ibis there is a distinct difference. Moreover, the few breaks prior to 1940 are ignored -- this is because of some uncertainty in identification, as breaks prior to 1940 are not given key names in our records.

(2) Breaks Excluded On the principle of only including named keys in the list, breaks of numbered groups, NOT-keys, Barnyards and County keys have been excluded (except in a few cases where e.g. a numbered group has since the first break been given a definite name). Rocket I and Tricycle breaks are also omitted -- the former because Rocket I is being dealt with in Mr. Twinn's History, the latter because Tricycle keys were never recognised as proper Hut 6 keys and were eventually taken over by Mr. Twinn's section. Furthermore, suffixes(which on Air keys at least meant usually a replacement of a compromised key) are not regarded as a different key - i.e. no separate account is taken of Red II, Gadfly IIA and the like. On Army keys I and II are naturally counted as different, but no account is taken of III, etc. which could merely indicate a replacement, except, of course, in such clear cases as Chaffinch III and Kestrel III which were quite distinct keys. These omitted breaks are very numerous indeed, particularly in the last year of the war: had they all been included, the following list would have been double its present length.

(3) Breaks Included The breaks include breaks by capture -- this is sometimes mentioned in the last column, but not necessarily always. This list was compiled from our keybooks which made no separate mention of captured keys.

(4) Composite Breaks During 1943 it was discovered that certain normally separate keys were using the same machine settings for a month at a time. Such composite breaks are here only reckoned as new if none of the components had previously been broken. If a composite break is reckoned, later independent breaks of one component are not reckoned as new.

(5) Comment Under this head there are only inserted points of special interest with regard to number of breaks or duplication of a key name. More general details of the key must be sought in the separate key histories or in the lists of Air and Army keys identified that will be found at the end of Book 3.

(6) Authority The authority from which this list is compiled is the series of keybooks kept currently by Hut 6 -- ultimately the sole authority on such matters. It is thus almost inevitable that any errors made in this current record -- e.g. in identification or naming of keys -- will be transferred to the present list, but the wholesale exclusion of unnamed keys does at least remove the most doubtful category.

TABLE OF FIRST BREAKS OF KEYS

	Date	Key Name	Comment
1.	Jan. 6, 1940	Red	
2.	" 18, "	Green	Later called Greenshank
3.	" 29, "	Blue	
4.	Apr. 10, "	Yellow	
5.	May 26, "	Purple	Not broken again
6.	Sept. 2, "	Brown	
7.	Dec. 10, "	Orange	
8.	" 24, "	Violet	
9.	Feb. 28, 1941	Light Blue	
10.	Mar. 26, "	A.F.5	Later called Chaffinch
11.	May 8, "	Onion	
12.	June 27, "	Vulture	
13.	" " "	Mustard	
14.	July 9, "	Kestrel	Later split into four keys as under
15.	" 31, "	Leek	
16.	Aug. 10, "	Kestrel III	
17.	" 16, "	" I	
18.	" 20, "	" II	
19.	Oct. 21, "	Vulture II	
20.	Nov. 12, "	Chaffinch II	
21.	" 14, "	" I	
22.	" 23, "	Phoenix	By capture
23.	" 27, "	Kestrel IV	
24.	Dec. 1, "	Orange II	
25.	" 17, "	Brown II	
26.	Jan. 1, 1942	Hornet	First day of key's existence
27.	" " "	Wasp	"
28.	" " "	Pink	
29.	" " "	Gadfly	First day of key's existence
30.	" 2, "	Kite	
31.	" 7, "	Cockroach	
32.	" 12, "	Foxglove	
33.	" " "	Locust	
34.	" 17, "	Primrose	
35.	" 22, "	Gannet I	Not broken again
36.	Feb. 20, "	Raven III	Not broken again
37.	Mar. 3, "	Orange III	
38.	" 4, "	Beetle	
39.	" 8, "	Raven I	
40.	Apr. 7, "	Snowdrop	
41.	" 8, "	Garlic	
42.	" 13, "	Chaffinch III	
43.	" 22, "	Scorpion	
44.	May 9, "	Daffodil	
45.	" 11, "	Raven II	
46.	" 18, "	Skylark	
47.	June 8, "	Mosquito	
48.	" 16, "	Skunk	
49.	July 15, "	Weasel	
50.	" 23, "	Thrush	
51.	Aug. 10, "	Narcissus	
52.	" 14, "	Quince I	
53.	" 24, "	Rook I	Not broken again

ARKER. T
: FROM

TABLE OF FIRST BREAKS OF KEYS (Continued)

	Date		Key Name	Comments
54.	Sept.	2, 1942	Celery	
55.	"	24, "	Crab	
56.	"	30, "	Osprey	
57.	Nov.	20, "	Bullfinch	
58.	"	28, "	Mallard	
59.	Dec.	2, "	Goldfinch	Really Bullfinch A
60.	"	16, "	Robin	Not broken again
61.	"	31, "	Brown "S"	
62.	Jan.	2, 1943	Hawfinch	Really Chaffinch I
63.	"	8, "	Dodo	
64.	"	21, "	Porcupine	
65.	Feb.	10, "	Bullfinch II	
66.	"	12, "	Merlin	
67.	"	13, "	Nuthatch	Called at the time K/8738
68.	"	21, "	Hedgehog	
69.	"	22, "	Falcon I	
70.	"	25, "	Ermine	
71.	Mar.	1, "	Orchid+Tulip+Clover	
72.	"	5, "	Dragonfly	
73.	"	9, "	Shamrock	
74.	Apr.	6, "	Sparrow	
75.	May	1, "	Lily	
76.	"	8, "	Cormorant	Only broken a few times
77.	"	12, "	Aster	
78.	"	13, "	Lobster	
79.	"	16, "	Buzzard	
80.	June	2, "	Albatross	
81.	"	" "	Albatross II	
82.	"	14, "	Lion	
83.	"	30, "	Mayfly	
84.	July	3, "	Squirrel	
85.	"	23, "	Puffin II	Called at the time Puffin
86.	Aug.	1, "	Puma	
87.	"	2, "	Gannet II	
88.	"	4, "	Sheep	Really Primrose B
89.	"	13, "	Dingo	
90.	"	23, "	Shrike I	
91.	"	24, "	Peregrine	
92.	Sept.	2, "	Goshawk	Later found to equal Kite
93.	"	9, "	Firefly	
94.	"	13, "	Poppy	
95.	"	15, "	Puffin I	Called at the time Jay
96.	"	18, "	Wryneck I	
97.	"	20, "	Gorse	
98.	"	22, "	Brown III	
99.	Oct.	3, "	Indigo	
100.	"	" "	Shrike II	
101.	"	11 onwards	Brown IV	
102.	"	13, 1943	Stork	
103.	"	22, "	Yak	
104.	"	23, "	Quince II (Italian)	See section on "The S.S. Keys"
105.	Nov.	16, "	Leveret	
106.	"	" "	Woodpecker	
107.	"	29, "	Magpie	Not broken again
108.	Dec.	15, "	Bullfinch (Italian)	See section on "The Italian Army Keys"

TABLE OF FIRST BREAKS OF KEYS (Continued)

	Date			Key Name	Comments
109.	Jan.	31,	1944	Wryneck II	
110.	Feb.	9,	"	Llama	
111.	"	10,	"	Roulette I	
112.	"	5,	"	Leopard	
113.	"	11,	"	Jaguar	
114.	"	14,	"	Owl	
115.	"	27,	"	Chicken I	
116.	Mar.	1,	"	Bantam I	
117.	"	3,	"	Owl II	
118.	"	5,	"	Wagtail	
119.	"	17,	"	Nightjar	
120.	"	23,	"	Cornerake	
121.	"	27,	"	Pelican	
122.	Apr.	1,	"	Quince II	
123.	"	"	"	Pumpkin	
124.	"	3,	"	Coot	Possibly the same as Kite
125.	"	17,	"	Avocet	
126.	"	24,	"	Cricket	
127.	May	1,	"	Gnat	
128.	"	30,	"	Bantam II	
129.	"	"	"	Kingfisher II	
130.	"	31,	"	Ocelot	
131.	June	6,	"	Medlar	
132.	"	9,	"	Duck I	
133.	"	"	"	Duck II	
134.	"	"	"	Armadillo	By capture
135.	"	11,	"	Raccoon	
136.	"	"	"	Pullet	
137.	"	13,	"	Cress	
138.	"	15,	"	Penguin	
139.	"	16,	"	Platypus	
140.	"	19,	"	Peewit	
141.	"	29,	"	Kingfisher	
142.	July	5,	"	Jerboa	
143.	"	7,	"	Nightjar II	
144.	"	16,	"	Glowworm	
145.	Aug.	1,	"	Emu I	
146.	"	"	"	Emu II	
147.	"	2,	"	Chipmunk	Not broken again
148.	"	3,	"	Flamingo	
149.	"	6,	"	Blunderbuss	Called at the time Rocket II
150.	"	10,	"	Dodo II	
151.	"	21,	"	Grapefruit	Not broken again
152.	Sept.	5,	"	Gorilla	
153.	"	8,	"	Gosling	
154.	"	12,	"	Quail	Called at the time Vulture G
155.	Oct.	2,	"	Lorient	
156.	"	"	"	Culverin	Called at the time Stephenson
157.	"	5,	"	Falcon II	
158.	"	10,	"	Pigeon	
159.	"	16,	"	Diver	
160.	"	21,	"	Sparrow I	
161.	"	"	"	Sparrow II	
162.	Nov.	2,	"	Quail II	
163.	"	8,	"	Egret	
164.	"	21,	"	Flycatcher	
165.	"	28,	"	Ibis	
166.	Dec.	1,	"	Wallflower	

TABLE OF FIRST BREAKS OF KEYS (Continued)

	Date			Key Name	Comments
167.	Dec.	2,	1944	Gentian	
168.	"	8,	"	Avocet II	
169.	"	10,	"	Violet	Not same key as Violet of 1940 - 1
170.	"	15,	"	Chimpanzee	
171.	Jan.	15,	1945	Whimbrel	
172.	Feb.	1,	"	Oriole	Not broken again
173.	"	16,	"	Roulette III	"
174.	Mar.	1,	"	Grouse	By capture
175.	"	"	"	Marmoset	"
176.	"	14,	"	Plum	
177.	"	17,	"	Hummingbird	
178.	Apr.	11,	"	Moth	
179.	"	23,	"	Monkey	
180.	"	26,	"	Whinchat	
181.	"	28.	"	Goat	

3·93 ENGLISH KEY NAMES OF AIR AND ARMY KEYS

3·930 The Early Days

In the early days of Hut 6 the number of Air and Army groups intercepted was so small that the provision of English covernames was a very minor problem. As soon as the continuity of a group was established it was named after a colour; thus the G.A.F. groups in December 1939, were Red and Blue, the Army group, Green. Colour names were chosen because messages could then be identified by marking them with correct coloured pencil. Before a definite long-term continuity had been established groups were distinguished by frequency names, e.g. E/4700 Group, E/5420 Group. Certain groups, because their function was known, were given a purely functional name, e.g. Police, Railway, A.F.5 (Army Formation 5).

This method of naming was considered adequate until early in 1941, but by this time the number of keys had already greatly increased and the extension of the North African and Russian theatres promised many more. The position was carefully reviewed and the authority for naming all Hut 6 keys vested in a single individual, whose task it was to keep liaison with other sections to prevent any possible confusion arising from the duplication of key names. Later a central G.C.C.S. authority was set up and the naming of Hut 6 keys became part of its commitment. The realms of Ornithology were allotted to the Army and bird names became the distinguishing mark of Army keys until the end of the war. Air keys were more strictly categorised, the divisions being distinguished by the names of colours, flowers, vegetables, insects, mammals and jungle animals.

3·931 Air Keys

(a) Colours Colour names were retained for G.A.F. keys of the "general" class. At the time of the change there were only Red, Blue, and Pink, though later it was necessary to add Indigo and Puce. The old Army key, Green, was renamed Greenshank, but Brown, the key of the "beam bombers", retained its original name, partly for sentimental reasons, but mostly because source information had been passed on for some time under that name and confusion in intelligence circles might have resulted from a change.

(b) Flowers Flower names were given to the Luftgau keys because the principal Luftgau key had formerly been called Violet - a colour name.

(c) Vegetables Vegetable names were allotted to the weather keys and also to certain technical keys such as Mustard, the key of the G.A.F. Y Service.

Flowers and Vegetables were the two earliest categories, but later it became necessary to add:

(d) Insects Insect names were given to Fliegerkorps keys, introduced by the Germans in January 1942.

(e) Mammals Mammal names were reserved for Geschwader keys, which had a most disconcerting habit of appearing and disappearing again at short notice, a trait which made the correct identification and naming of such keys a rather tricky business.

(f) Jungle Animals The names of jungle animals were assigned to the Luftflotte keys, a fairly late key division in the G.A.F. The choice of this type of key name arose in the following manner. A key appeared in Norway on the stars of Fliegerführer Luftflotte 5 and was named Lobster to bring it into line with the only other known Fliegerführer key, Scorpion, the key of Fliegerführer Afrika. (Fliegerführer keys as such were never distinctly recognised as a separate category since they were Sonderschlüssel and when later two more Fliegerführer keys appeared they were called Yak and Llama, names having no relation to Scorpion.) The name Lobster was objected to by the Naval Section on the grounds that it would lead to confusion with their "marine" classes for naval keys. About the same time it was discovered that Lobster had a wider scope than was originally thought and was in fact more likely to be the key of Luftflotte 5 itself. The name was therefore altered to Lion and a new key category started.

There were certain exceptions to the system as it has been outlined above, for, although this was in essence the theoretical basis upon which all G.A.F. keys were named, in practice various inconsistencies developed, the result either of identification to the wrong category by us, or a German alteration in the status of a unit after its key had received an English covername. In either case it was difficult to change an established name without threatening to disrupt intelligence continuity. In all fairness to those responsible for identifying keys, it should be noted that discrepancies were for the most part the result of German changes and not of misidentification. The two examples which follow will make the exact nature of the problem clearer.

(1) When the system of nomenclature was originally drawn up all Luftflotten used Red, the general key. In January 1942 the key of Fliegerkorps I, in the North Prussian sector, was named Mosquito, but in July of the same year Fliegerkorps I was transferred to the south and given the title of Luftwaffen Kdo. Don. As, however, it left its key, callsigns, and frequencies behind with Luftflotte 1, it was necessary to retain the name Mosquito in the north and introduce a new name, Ermine, in the south. The matter was later further complicated by the fact that in February 1943 Luftwaffen Kdo. Don. reverted to its old status and was again known as Fliegerkorps I. This meant that, by then, both Mosquito and Ermine were inconsistent, as regards name categories, with the original schedule; they remained so to the end of the war.

(2) The key known as Skunk when it first appeared was on a Geschwader network and was named on that basis. Later it was shown that the key was really the property of Fliegerkorps VIII, but at the special request of Hut 3 the name was retained.

When on February 1, 1945 the Germans introduced changing frequencies and encoded callsigns in the G.A.F., it was realised that some new system of temporary nomenclature would have to be introduced to deal with groups for which a discriminant repeat had been established but which were otherwise unidentified. It was decided to issue such predictions under "County" names, i.e. E/York, E/Kent, to the stations and Sixta until a more definite identification could be suggested on the strength of new source and W/T evidence. The supposition was that such names would be shortlived, but in actual practice it soon became apparent that many of the groups (or keys) so named were "new" keys in the sense that they had no counterpart under the old key categories. They

were in fact mainly keys issued by local units to bridge gaps in key distribution caused by the general disorganisation of the German lines of communication during the last few months of the war. English county names were used for the month of February, Scottish for March, American states (by a polite extension of the term) for April, and Irish for May.

The use of numeral and letter suffixes with Air key names requires a word of explanation. With very few exceptions (e.g. Brown I, II and III: Mustard I and II) Roman numerals were used to distinguish the Ersatz key from the Gebrauch in the case of a compromise (Jaguar I = Gebrauch key; Jaguar II = Ersatz key). Letter suffixes were used as follows: A = last month's key (i.e. Jaguar of March used in April = Jaguar A); B = Ersatz key of current month likely to be used as Gebrauch key of following month ; C = either a compromised current key, or the key intended as the Ersatz of the following month used as the Gebrauch key of the current month; X = any key used in a hatted order.

3·932 Army Keys

It has been stated that Army key nomenclature was based wholly on bird names. In the following discussion, however, the S.S. keys and the Railway keys are, for the sake of compactness, being considered in the same category.

Although all Army keys were named under the single category of bird names, there was some attempt made to associate keys in certain areas with definite classes of birds. For example, birds of prey were used for the Eastern Front (e.g. Vulture, Kite, Kestrel) and "Barnyard" names for the Western Front (e.g. Duck, Bantam, Chicken).

It must be observed in connection with Army key nomenclature that certain types of key (Armee, Heeres, Wehrmacht) had two or more "versions"; one, the M/S for Geheim traffic; two, the Stabs M/S for Geheimekommandosache or Chefsache; and three, rarely used, the O.K.H. or Offizier key, the highest grade Enigma Army key. As it would only have complicated matters to have assigned a different name to each "version", it became the convention to refer to them as I, II and III respectively (e.g. Puffin I, Puffin II and Puffin III). Various exceptions to this general rule crept in from time to time, so that I and II following an Army key name might occasionally have reference to some purely functional association (e.g. Osprey I and II and the Railway key, Rocket I and II). An attempt was made, however, to remove the confusion wherever possible, unless the type of key involved (as in Rocket I and II) made any real confusion unlikely. The Army use of Roman numerals with key names must thus be sharply distinguished from Air usage.

The first S.S. key, intercepted from early in 1939, was finally named Orange in April 1940. It was thus originally a colour key. With the appearance of other S.S. keys, however, it was found more constructive to look upon Orange as a fruit and to name the other S.S. keys by fruit names (e.g. Quince, Medlar, Apple).

The key originally knows as Railway retained its name until October 1943, when it became Rocket. As Rocket, however, soon after became paired with another Railway key called Stephenson, it was considered that the association was too obvious to be secure. As a result the railway keys were renamed after weapons

(e.g. Culverin, Blunderbuss), Rocket retaining its original name as being equally proper in the new category.

The key known as T.G.D., probably the key of the Reichssicherungsdienst, was named from one of its early fixed callsigns, a name which was left as undisturbed as the key was unbroken throughout the war.

Towards the close of the war, when the tide was turning more and more seriously against the Germans, two types of special key were brought into common use in both G.A.F. and Army. The first, Sondermaschinenschlüssel, already noticed in the discussion of "County" covernames in the Air, likewise appeared in the Army and were most usually allotted to isolated units garrisoning Fortresses; the second, NOT-keys were for units, both Air and Army, in similar circumstances or for units with no other machine key available. Sondermaschinenschlüssel were in all respects quite normal keys, but, as their days of validity were generally considered to be numbered, they did not, if Army, receive a bird name but were distinguished by geographical location (e.g. E/Lorient, E/Dunkirk). In the Air the use of County names has already been noted, and before February 1st covernames based on frequency were quite usual. If, however, any Air or Army Sonder key was expected to function permanently, it was given a regular covername (e.g. Armadillo, a Flugssicherungs key; Cornerake, the key of P.W. Kdo. II).

NOT-keys, both in the Air and Army, were named from their single discriminant (e.g. NOT/HNG). There was one exception to this rule, NOT/Guernsey.